IN THE CLAIMS:

1. (Currently Amended) A method, comprising:

receiving, in a secure environment in a terminal, via a secure channel established by an installation part of an application previously stored in said terminal outside said secure environment, from a server outside said terminal, a first key for decrypting an encrypted part of said application;

loading said encrypted part of said application from storage outside said secure environment into said secure environment;

decrypting, in the secure environment, said encrypted part of said application by means of said first key for execution in said secure environment;

re-encrypting, in said secure environment, the application by means of a second key; and

storing, outside said secure environment, the re-encrypted part of said application.

2. (Currently Amended) A method, comprising:

~~receiving~~storing an ~~encrypted~~ application outside a secure environment in a terminal;

receiving, in ~~a~~said secure environment in said terminal, via a secure channel established by an installation part of said application, from a server outside said terminal, a first key for decrypting ~~said~~an encrypted part of said application;

loading said encrypted part of said application from storage outside said secure environment into said secure environment for decryption by said first key and execution in said secure environment;

encrypting, in said secure environment, said first key by means of a second key; and

storing, outside said secure environment, the encrypted first key.

3. (Previously Presented) The method according to claim 1, the method comprising:

encrypting, in said secure environment, said first key by means of the second key; and

storing, outside said secure environment, the encrypted first key.

4. (Previously Presented) The method according to claim 1, wherein said second key is symmetric and can be derived from the application.

5. (Currently Amended) The method according to claim 4, wherein said second key is comprised in the encrypted part of said application ~~itself~~.

6. (Previously Presented) The method according to claim 4, wherein said second key is generated in the secure environment using an application seed.

7. (Original) The method according to claim 1, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

8. (Currently Amended) Apparatus, comprising:

a processor; and

a memory including computer program code, the memory and the computer program code configured to, with the processor, cause the apparatus at least to:

~~an application including an installation part for receiving,~~receive in a secure environment of ~~a terminal~~said apparatus, via a secure channel established by an installation part of an application previously stored in said apparatus outside said secure environment, from a server outside said ~~terminal~~apparatus, a first key for decrypting an encrypted part of said application;

~~a processor for decrypting~~load said encrypted part of said application from outside said secure environment into said secure environment and decrypt, in the secure environment, said encrypted part of said application by means of said first key for execution in said secure environment;

~~said processor for re-encrypting~~re-encrypt, in said secure environment, the application based on a second key decrypted from said encrypted part of said application; and

~~a memory for storing~~store in said apparatus, outside said secure environment, the re-encrypted application.

9. (Currently Amended) Apparatus, comprising:

a processor; and

a memory including computer program code, the memory and the computer program code configured to, with the processor, cause the apparatus at least to:

~~an application including an installation part for receiving~~receive, in a secure environment of ~~a terminal~~said apparatus, via a secure channel established by an installation part of an application previously stored in said apparatus outside said secure environment, from a server outside said ~~terminal~~apparatus, a first key for decrypting an encrypted part of said application;

load said encrypted part of said application from storage in said apparatus outside said secure environment into said secure environment for decryption by said first key and for execution in said secure environment;

~~a processor for encrypting~~encrypt, in said secure environment, said first key by means of a second key; and

~~said processor for storing~~store in ~~a memory of~~ said ~~terminal~~apparatus, outside said secure environment, the ~~encrypted~~ first key encrypted by the second key.

10. (Currently Amended) The apparatus according to claim 8, wherein said ~~processor is~~memory and the computer program code are configured to, with the processor, cause the apparatus to:

~~for encrypting~~encrypt, in said secure environment, said first key by means of the second key; and

~~for storing~~store in said apparatus, outside said secure environment, the encrypted first key.

11. (Previously Presented) The apparatus according to claim 8, wherein said second key is symmetric and can be derived from the application.

12. (Currently Amended) The apparatus according to claim 11, wherein said second key is comprised in the encrypted part of said application ~~itself~~.

13. (Previously Presented) The apparatus according to claim 11, wherein said second key is generated in the secure environment using an application seed.

14. (Previously Presented) The apparatus according to claim 8, wherein the apparatus is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

15. (Previously Presented) The method of claim 2, wherein said second key is symmetric and can be derived from the application.

16. (Currently Amended) The method of claim 15, wherein said second key is comprised in the encrypted part of the application ~~itself~~.

17. (Previously Presented) The method of claim 15, wherein said second key is generated in the secure environment using an application seed.

18. (Original) The method of claim 2, wherein multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

19. (Previously Presented) The method of claim 9, wherein said second key is symmetric and can be derived from the application.

20. (Currently Amended) The method of claim 19, wherein said second key is comprised in the encrypted part of the application ~~itself~~.

21. (Previously Presented) The method of claim 9, wherein the apparatus is arranged such that multiple keys can be transferred successively on the secure channel into the secure environment, each key being used to decrypt a corresponding encrypted application in the secure environment.

22. (Currently Amended) A terminal device comprising:

a processor; and

a memory including computer program code, the memory and the computer program code configured to, with the processor, cause the terminal device at least to:

~~an installation part of~~load an encrypted application~~, responsive to~~ into a secure environment of said terminal device; and

decrypt said encrypted application in said secure environment using a first key provided over a secure channel from a server external to said terminal device ~~for providing said first key; and~~

~~a secure environment, responsive to said first key from said installation part of said application for decrypting an encrypted application in said terminal device using said first key received over said secure channel from said server external to said terminal device~~.

23. (Currently Amended) The terminal device of claim 22, wherein said first key is encrypted by said server using a ~~second~~public key belonging to said terminal device for providing said first key from said server to said terminal device for decryption of said first key by a private key of said terminal device in said secure environment of said terminal device.

24. (Currently Amended) An integrated circuit for installation in a terminal comprising ~~a signal processor and~~ a secure environment, said secure environment responsive to a first key from a server outside said terminal received over a secure

channel for decrypting ~~an encrypted application~~ within said secure environment an encrypted application loaded from an insecure environment in said terminal, for executing said decrypted application within said secure environment and for encrypting said first key with a second key belonging to said terminal device for storage in said terminal outside said secure environment so that said first key can be used again within said secure environment without need for receipt again of said first key from said server.

25. (Previously Presented) The method of claim 2, further comprising

receiving another encrypted application in the terminal;

loading the encrypted first key from outside said secure environment;

decrypting the encrypted first key with the second key; and

decrypting the other encrypted application with the decrypted first key.

26. (Previously Presented) The method of claim 25, further comprising:

re-encrypting the first key by means of the second key; and

storing, outside said secure environment, the encrypted first key.

27. (Currently Amended) The apparatus of claim 9, wherein said ~~installation part is for receiving another encrypted application in the terminal and wherein said processor is configured~~memory and the computer program code are configured to, with the processor, cause the apparatus to:

load the encrypted first key from outside said secure environment;

decrypt the encrypted first key with the second key; and

decrypt ~~the other~~with the decrypted first key another encrypted application ~~with the decrypted first key~~loaded into the secure environment.

28. (Currently Amended) The apparatus of claim 27, wherein said ~~processor is further configured~~memory and the computer program code are configured to, with the processor, cause the apparatus to:

re-encrypt the first key by means of the second key; and

store, outside said secure environment, the encrypted first key.

29. (Previously Presented) The method of claim 7, further comprising:

encrypting, in said secure environment, each of said multiple keys by means of the second key; and

storing, outside said secure environment, each of the multiple keys encrypted by the second key.

30. (Previously Presented) The method of claim 29, further comprising:

receiving a plurality of encrypted applications in the terminal and storing same outside said secure environment;

loading one of said plurality of encrypted applications into the secure environment;

loading a corresponding one of said plurality of encrypted multiple keys stored outside said secure environment into said secure environment;

decrypting the corresponding encrypted key by means of the second key; and

decrypting the loaded encrypted application by means of the decrypted corresponding key.

31. (Currently Amended) The apparatus of claim 14, wherein said ~~processor is configured~~memory and the computer program code are configured to, with the processor, cause the apparatus to:

encrypt, in said secure environment, each of said multiple keys by means of the second key; and

store, outside said secure environment, each of the multiple keys encrypted by the second key.

32. (Currently Amended) The apparatus of claim 31, wherein said ~~apparatus is configured~~memory and the computer program code are configured to, with the processor, cause the apparatus to:

receive a plurality of encrypted applications;

to store same outside said secure environment;

to load a selected one of said plurality of encrypted applications into the same environment;

load a corresponding one of said plurality of encrypted multiple keys stored outside said secure environment into said secure environment;

decrypt the corresponding encrypted key by means of the second key; and

decrypt the loaded selected encrypted application by means of the decrypted corresponding key.